



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/776,407	02/10/2004	Steven A. Crosson Smith	BT-024	2424
29956	7590	12/19/2005	EXAMINER	
TIMOTHY P. O'HAGAN			AUGUSTIN, EVENS J	
8710 KILKENNY CT				
FORT MYERS, FL 33912			ART UNIT	PAPER NUMBER
			3621	

DATE MAILED: 12/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/776,407	CROSSON SMITH, STEVEN A.
	Examiner	Art Unit
	Evens Augustin	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 28 November 2005.
 2a) This action is FINAL. 2b) This action is non-final.-
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1,5-8,11 and 12 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1,5-8,11 and 12 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____

Status of Claims

1. Claims 1, 5-8 and 11-12 have been examined.

Response To Arguments

2. The USPTO has fully considered the applicant's arguments with regard to the characteristics of the prior art, vis-à-vis the claimed invention, but has not found those arguments to be persuasive. Applicant stated the prior art failed to show that authorization is executed at a remote system. Specifically, Linehan shows the authentication is taken place in a remote system via the internet (column 7, lines 55-67, column 8, lines 1-15, column 15, lines 59-67, column 16, lines 1-24).
3. In light of the applicant's specification, the replacing the digest dummy data with the real data is interpreted as a hash function in which a message is hashed. According to Candelore, authentication can be performed by either XORing the authentication information with hash of the clear text data blocks to produce a verification value that is subsequently compared to a pre-stored value, or the authentication information can be simply compared to the hashed program information (column 13, lines 20-25). If a pirate changes any data in preceding blocks in the chain for trialing, the computed hash data that is compared with the authentication information will be incorrect, and the resulting verification value will not match (column 12, lines 7-10). According to Candelore et al., the dummy is authenticated just like the any other data in the process (column 23, lines 38-58).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 5-8 and 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linehan (U.S 6327578) in view of Candelore et al. (U.S 6061449)

As per claims 1, 5-8 and 11-12, Linehan discloses an invention that includes the step of sending from a consumer's computer a start message over an Internet network to a merchant's computer. The merchant's computer then replies to the consumer's computer with a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank. The computer invention comprises of the following:

- A merchant generating an authorization request which includes containing payment amount, order description, timestamp, a random nonce, and possible additional data depending upon requirements (column 9, lines 35-40). The authorization request can also include a hash of an order description instead of the actual order description (column 16, lines 18-25)
- The authorization request or hash is transferred to a remote system (column 14, lines 28-31)
- Once the authorization request/hash is sent to consumer computer, the request gets sent to consumer's/issuing bank and verifies the merchant's signature to prove that the consumer

is dealing with the actual merchant and validates the merchant's certificate and the acquirer's certificate (column 6, lines 8-12, column 15, lines 25-32)

- Sending over the Internet network an authorization token, an issuer's digital certificate, and a reference to the consumer's credit or debit card number. The authorization token includes the payment amount, order description, timestamp, a random nonce, the merchant identifier from the merchant's digital certificate, and the acquiring bank identifier from the acquiring bank's digital certificate, plus a reference to the consumer's credit or debit card number (column 25, lines 36-44)
- The merchant presenting the authorization code to a payment processor in order to complete the transaction (column 6, lines 48-55, column 16, lines 6-8)
- The authorization includes a combination of payment amount, order description, timestamp, a random nonce, and possible additional data depending upon requirements (column 9, lines 35-40). The authorization request can also include a hash of an order description instead of the actual order description (column 16, lines 18-25)
- The system can also generate dummy data (column 11, lines 3-9), in combination with the payment amount, order description, timestamp, a random nonce, the merchant identifier from the merchant's digital certificate, and the acquiring bank identifier from the acquiring bank's digital certificate, plus a reference to the consumer's credit or debit card number (column 25, lines 36-44)
- The system also used challenge-response authentication system between the remote computer and the server (column 7, lines 25-33)

Although Linehan teaches the aspects of generating dummy data for the purpose/functionality of authentication, Linehan did not explicitly describe a method in which the dummy data is being authenticated and going through the encryption process.

However, Candelore et al. describe an invention that relates to an apparatus for efficiently and securely transferring blocks of program information between a secure circuit and an external storage device. Candelore et al. teach an invention in which encrypted, authenticated information and dummy data are securely communicated between an external memory and a cryptographic ASIC in cipher block chains (column 17, lines 61-64). Modern cryptographic applications often employ public key cryptography, which generally require larger keys than secret key cryptography. The scrambling sender or descrambling receiver may perform some type of cryptographic application which may interface on an open network such as the Internet, which may require the storing of a number of various public keys, e.g., from a Root Authority, or Certificate Authority (column 8, lines 65-67, column 9, lines 1-6). If a pirate changes any data in preceding blocks in the chain for trialing, the computed hash data that is compared with the authentication information will be incorrect, and the resulting verification value will not match (column 12, lines 7-10). According to Candelore et al., the dummy is authenticated just like the any other data in the process (column 23, lines 38-58).

Therefore, in view of Candelore et al.'s teaching, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to combine Linehan's invention in view of Candelore et al. for authenticating dummy data just like any other data in the process. It would have been obvious to one skilled in the art to authenticate dummy data because it would confuse the pirate attempting to analyze the authenticated data (column 23, lines 53-55).

Conclusion

6. *Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that if the applicant is preparing to respond, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.*

Art Unit: 3621

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- **Doggett et al. (US 5677955)** - An electronic instrument is created in a computer-based method for affecting a transfer of funds from an account of a payer in a funds-holding institution to a payee. The electronic instrument includes an electronic signature of the payer, digital representations of payment instructions, the identity of the payer, the identity of the payee, and the identity of the funds-holding institution
- **Wheeler et al. (US 6915430)** - The present invention generally relates to electronic communications and, in particular, to devices that generate digital signatures associated with electronic communications

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Evens Augustin whose telephone number is 571-272-6860. The examiner can normally be reached on Monday thru Friday 8 to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim Trammel can be reached on 571-272-6712.

Any response to this action should be mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is 571-272-6584.

Evens J. Augustin
December 9, 2005

JAMES P. TRAMMEL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600